KRIVIČNO - PRAVNA ZAŠTITA SISTEMA KRITIČNE INFRASTRUKTURE

CRIMINAL - LEGAL PROTECTION OF THE CRITICAL INFRASTRUCTURE SYSTEM

Pregledni naučni članak

Edin Garaplija[*]

Sažetak

Prepoznavanje potrebe da se na nacionalnom i lokalnom nivou najprije uspostavi savremena zakonodavno-pravna legislativa, daje osnovne temelje za uspostavu efikasnije i pravovremene zaštita objekate i sistema kritične infrastructure. Ovakav pristup podrazumjeva izgradnju integrisanog sistema zaštite i spašavanja, uz njegovu potpunu digitalizaciju, koju mora pratiti "cyber sigurnost" cjelokupnog sistema. Legislativa koja tretira ovu oblast, a posebno ona koja tretira aspekt njene krivično-pravne zaštite, mora se hitno uspostaviti i kontinuirano unaprijeđivati, kako bi uspješno pratila sofisticiranost metoda i sredstava za počinjenje krivičnih dijela koja se tiču ugroza sistema i objekata kritične infrastrukture. Po svom obimu, namjeri i definiciji, više je različitih vrsta ovih krivičnih dijela, od kojih ćemo ovdje obraditi krivično-pravne aspekte onih najtežih i načešćih, krivičnih dijela terorizma, krađe i vandalizma, sabotaže i špijunaže. Ova krivična dijela mogu biti izazvana vanjskim ali i unutrašnjim destruktivnim uticajem, različitim pobudama namjere, te po svome obimu mogu djelimično ili trajno oštetiti sisteme i objekte kritične infrastrukture, ugroziti živote i zdravlje ljudi, imovinu i životnu sredinu.

Ključne riječi: krivično pravo, zaštita, kritična infrastruktura.

[*] Doktorant Fakulteta za kriminalistiku, kriminologiju i sigurnosne studije, Univerzitet u Sarajevu, Institut za upravljanje rizicima i naučnoistraživački rad, Sarajevo/Beograd/Podgorica, e-mail: edingaraplija@fkn.unsa.ba

Abstract

Recognizing the need to first establishing of modern legislative and the legal regulative at the national and local level, provides the basic foundations for the establishment of more efficient and timely protection of facilities and critical infrastructure systems. This approach implies the construction of an integrated protection and rescue system, with its full digitalization, which must be accompanied by "cyber security" of the entire systems. Legislation dealing with this area, and especially that dealing with the aspect of its criminal law protection, must be urgently established and continuously improved, in order to successfully monitor the sophistication of methods and means of committing crimes related to threats to critical infrastructure systems and facilities. According to their scope, intention and definition, there are several different types of these crimes, of which we will deal with the most serious and common criminal-legal aspects of the criminal acts of terrorism, theft and vandalism, sabotage and espionage. These crimes can be caused by external as well as internal destructive influence, various motives of intent, and by their scope can partially or permanently damage systems and facilities of critical infrastructure, endanger human lives and health, property and the environment.

Key words: criminal law, protection, critical infrastructure.

1. UVOD

Svijet svakodnevno pogađaju katastrofe, bilo das u one uzrokovane prirodnim fenomenima ili ljudskim nemarom ili namjerom. U njima stradaju ljudi, njihova imovina, priroda, kulturna i opšta dobra, regije, nacije i lokalna zajednica, a posebno kritična infrastruktura kao "žila kucavica" modernog društva. Koliko se god trudili da uspostavimo dobar i efikasan system prevencije i brzog odgovora na izazove prirodnih i drugih katastrofa, uvijek zakaže neka karika u ovom lancu, a najčešće je to ljudski faktor. Shodno tome, postavlja se pitanje odgovornosti onih koji svojim namjerama ili nemarom ugrožavaju zajednicu, njena materijalna i kulturna dobra, te njenu kritičnu infrastrukturu, odnosno onih koji su dužni da preventivno brinu o smanjenju rizika od katastrofa, a iz nekog razloga zakažu na tom zadatku. Globalne

klimatske promjene al ii globalna pandemija koji za sobom nose i svjetsku ekonomsku depresiju i sunovrat globalnih ali i nacionalnih ekonomija, nisu jedini rizici koji prijete Svijetu. Početkom mjeseca aprila 2020., serija požara je pogodila tlo Evrope, a među njima se posebno isticao katastrofalni požar u Ukrajini u blizini nekadašnje nuklearke "Černobil", koja je svojom havarijom 80-tih godina prošlog vijeka, već jednom u istoriji zaprijetila čovječanstvu. Prema izvještaju koji je objavio UNDRR* (UN office for Disaster Risk Reduction), ured Ujedinjenih Nacija (UN) za smanjenje rizika od katastrofa, u posljednjih dvadeset godina svijet je zahvatilo više od 7.000 registrovanih prirodnih katastrofa. Ured UN-a za smanjenje rizika od katastrofa (UNDRR) radi na preventivnom smanjenju rizika od katastrofa i gubitaka kako bi se osigurala održiva budućnost. UNDRR (ranije poznat kao UNISDR) je središnja tačka sistema Ujedinjenih naroda za smanjenje rizika od katastrofa i čuvar Sendai okvira, podržavajući zemlje i društva u provedbi, nadzoru i reviziji napretka. Mandat UNDRR-a je: „služiti kao središnja tačka u sistemu Ujedinjenih Naroda za koordinaciju smanjenja katastrofa i za osiguranje sinergije među aktivnostima smanjenja katastrofa sistema Ujedinjenih Naroda i regionalnih i nacionalnih organizacije i aktivnosti u socio-ekonomskim i humanitarnim oblastima." U izvještaju UNDRR-a, također stoji da je najviše stradalih u siromašnim zemljama s niskim i srednjim prihodima, gdje je poginulo čak 90% od ukupnog broja stradalih u prirodnim katastrofama na globalnom svjetskom nivou. Na samom vrhu te neslavne ljestvice nalazi se Haiti gdje je u posljednjih 20 godina od prirodnih katastrofa poginulo 230.000 ljudi ili 1/6 od ukupnog broja poginulih. Ban Ki-Moon, bivši glavni sekretar UN-a kazao je da je ovo strašan pokazatelj nejednakosti i klasnih podjela, koje vladaju na našem planetu zato što "bogate zemlje koje zahvati prirodna katastrofa plaćaju svoj danak velikom materijalnom štetom, a siromašne zemlje ljudskim životima". Najbolja ilustracija za ovu njegovu izjavu je činjenica da je upravo na Haitiju kojeg je zahvatio uragan Mathew, smrtno stradalo više od 1.000 ljudi, a u SAD-u samo desetak. To pokazuje da postoji izravna veza između socioekonomskog statusa zemlje i vjerojatnosti da se u toj zemlji smrtno strada u prirodnoj katastrofi, kazao je dr. Robert Glasser, čelni čovjek UNDRR-a. Govorio je i o primjerima stradavanja u katastrofalnim potresima te je naveo da je u Haitiju u 2010. godini u velikom potresu poginulo

* Mandat UNDRR-a definiran je nizom rezolucija Opće skupštine Ujedinjenih naroda, od kojih je najistaknutija: Rezolucija Generalne skupštine UN-a 56/195.

223.000 ljudi, no u isto tako jakom potresu u Čileu poginulo je mnogo manje ljudi, a u Novom Zelandu nitko. On smatra potpuno neprihvatljivim da zemlje u kojima vlada siromaštvo i loša vlast, i u kojima se jednom dogodila prirodna katastrofa, ostaju nepripremljene za neke buduće slične događaje. "No u zemlji poput Haitija to je jako teško postići, što zbog posvemašnjeg siromaštva, što zbog loše organizacije vlasti", kazao je Glasser. Dodao je da bi zemlja poput Haitija, uz obilnu pomoć međunarodne zajednice, trebala intenzivno raditi na sistemima za rano upozoravanje na nadolazeće katastrofe (poput uragana), na edukaciji stanovništva, ali i na poboljšanju kvalitete gradnje. "Smatram doista skandaloznim i neprihvatljivim da smo mi, izvan Haitija, mogli vidjeti oluju kako dolazi na televiziji dok je bilo nemoguće kontaktirati s ljudima na licu mjesta ranim upozorenjem ili, kad je ono poslano, ničemu nije poslužilo zbog nedostatne obuke stanovništva", istakao je Glasser. Svjedoci smo današnjice, da su klimatske promjene uzrok sve više prirodnih katastrofa poput: poplava, klizišta, toplinskih valova i snažnih oluja, koji su nakon potresa i tsunamija, najveće masovne ubojice čovječanstva[*].

Smanjenje rizika od nesreća (engl. Disaster Risk Reduction - DRR) predstavlja sistematičan pristup identifikaciji, procjeni i smanjenju rizika. Gledajući globalno, u vremenskom okviru od poslednjih 10-tak godina katastrofe uzlaznim trendom uzimaju veliki danak, a kao rezultat su imale presudni uticaj na sigurnost ljudi, zajednica i država u cjelini. Širom svijeta je preko 700 hiljada ljudi izgubilo živote, više od 1,4 miliona je povrijeđeno, a oko 23 miliona su ostala bez krova nad glavom. Više od 1,5 milijardi ljudi je pogođeno katastrofama na različite načine, uključujući žene, djecu i ranjive grupe ljudi te je ukupan ekonomski gubitak bio više od 1,3 triliona USD, dok je samo u poslednje dvije godine (2018. i 2019.) bilo preko 330 biliona USD ekonomskih gubitaka. U istom period je na globalnom nivou, 144 miliona ljudi raseljeno usljed ovih katastrofa[*]. U gore navedenim podacima nisu analizirane globalne ekonomske štete poruzočene svjetskom pandemijom COVID-19 ("koronavirus"), koje će zasigurno i industriju osiguranja i reosiguranja prisiliti na promjene u pristupu riziko-baziranim analizama u narednom periodu, te proširenju svoga portfolija na osiguranje lokalnih zajednica, organizacija i pojedinaca od budućih pandemijskih rizika. Sve ove prirodne i tehnološke

[*] UN DRR Global Assesment Report, https://gar.undrr.org/sites/default/files/reports/2019-05/full_gar_report.pdf (pristup: 20.03.2021.)

[*] Reosiguravajuća kuća Munich RE, NatCatSERVICE, https://natcatservice.munichre.com/ (14.04.2020.)

katastrofe, su dodatno uticale na ubrzanje klimatskih promjena, te značajno ugrozile globalni napredak ka održivom razvoju civilnog društva i državnih zajednica. Imajući u vidu gore izloženo, možemo zaključiti da se prirodne, tehničko-tehnološke i antropogene nesreće, nenamjerno i namjerno izazvane (terorizam), sve učestalije ponavljaju, globalno na svjetskom nivou i pogađaju, kako one najsiromašnije, tako i one na najvišem stepenu ekonomskog razvoja.

Shodno tome, prepoznavanje potrebe da se na nacionalnom i lokalnom nivou uspostavi savremena zakonodavno-pravna legislativa, daje osnovne temelje za uspostavu efikasnije i pravovremene zaštita objekate i sistema kritične infrastructure. Legislativa koja tretira prepoznavanje i zaštitu kritične infrastrukture, a posebno ona koja tretira aspekt njene krivično-pravne zaštite, mora se hitno uspostavljati i kontinuirano unaprijeđivati. Samo tako može uspješno pratila sofisticiranost metoda i sredstava za počinjenje krivičnih dijela koja se tiču ugroza sistema i objekata kritične infrastrukture.

2. KRIVIČNA DJELA TERORIZMA U SISTEMIMA I OBJEKTIMA KRITIČNE INFRASTRUKTURE

Da bi smo sagledali krivično pravne aspekte krivičnih dijela nastalih terorističkim aktima i napadima na objekte i sisteme KI, moramo najprije sagledati širi kontest nastanka pojma i definicije terorizma, kao globalnog destruktivnog fenomena. „Terorizam je jedno od najtežih krivičnih djela, kojim se ugrožavaju ne samo unutrašnji interesi i vrijednosti već i međunarodni mir i bezbjednost. Navedeni efekti i opasnost od terorizma su još više naglašeni posljednjih godina, što je uslovilo i promijenjen pristup u njegovom suzbijanju. U tom smislu, ovo krivično djelo je predmet normi krivičnog zakonodavstva duži niz godina. Ipak, eskalacija terorizma u posljednjih 30 godina uticala je na internacionalizaciju ovog fenomena. Čini se da je terorizam jedan od pojmova koji je najviše obuhvaćen međunarodnim pravom. To je uglavnom uticalo na jačanje krivičnopravne represije (propisivanje strožijih kazni) i povećanje broja terorističkih krivičnih djela. Tako su ova krivična djela u Bosni i Hercegovini sistematizovana u grupu krivičnih djela protiv čovječnosti i drugih vrijednosti zaštićenih međunarodnim pravom, a zaprijećena je i najteža kazna (dugotrajni zatvor). Pored osnovnog krivičnog djela terorizma, 2003. godine uvedeno je i novo krivično djelo – finansiranje terorističkih aktivnosti, koje je izmijenjeno 2015. godine, dok su 2010. godine uvedena još četiri teroristička krivična djela: javno podsticanje na terorističke aktivnosti,

vrbovanje radi terorističkih aktivnosti, obuka za izvođenje terorističkih aktivnosti i organizovanje terorističke grupe. Potom je 2014. godine inkriminisano (ne baš potpuno precizno i nedvosmisleno) učešće državljana BiH u stranim terorističkim aktivnostima putem krivičnog djela protivzakonito formiranje i pridruživanje stranim paravojnim ili parapolicijskim formacijama.“ (Simović, M., Šikman, M., 2017.)

Iako se pojam „terorizma“ danas povezuje sa vjerskim, najčešće „islamskim terorizmom“, kako ga definišu u pojedinim svjetskim centirma društveno-ekonomske moći, interesantno je da se terorizam pojavljuje još u doba vladavine starog rimskog carstva. Pa tako riječ terorizam (Klaić, B.,1978.), dolazi od latinske riječi teror, što označava strah, užas, zadavanje straha, izazivanje straha i trepeta, užasa, strave, jeze; primjena nasilja sve do fizičkog uništenja protivnika; strahovlada. Povijest terorizma seže od drevnih vremena, kada su već tada suparnici pokušali na razne načine, od zastrašivanja do tjelesnog nasilja, poraziti svoje suparnike. Jedna od prvih terorističkih skupina, o kojoj postoje provjereni povijesni podaci, operirala je na Bliskom istoku već u prvom stoljeću. Njezini su pripadnici bili Zeloti, židovski nacionalisti koji su se suprostavljali Rimskoj upravi nad Judejom. Zeloti su se prvi put pojavili u 6. godini prvog stoljeća, a ubrzo su nestali u podzemlju i započeli terorističke aktivnosti. Po gradovima i zemljama Judeje ubijali su Rimljane i Židove koji su priznavali rimsku vlast.

Još neke definicije ovog globalnog destruktivnog društvenog fenomena ističu slijedeće: "Terorizam je namjerno i sustavno ubijanje, sakaćenje i ugrožavanje nevinih kako bi se u njih utjeralo strah radi neke političke svrhe." (Harmon, C., 2002.) "Terorizam je specifičan oblik agresivnog djelovanja protiv naroda, životne sredine i materijalnih dobara neke zemlje u miru i u ratu." (Cvjetković, B., 2002.) Za čuvenog stručnjaka u borbi protiv terorizma Briana Jenkinsa definicija terorizma glasi: „Terorizam je upotreba ili prijetnja upotrebom sile, usmjerena na ostvarivanje političkih promjena.“ (Wise, R., J., 2020.) “Terorizam nije oblik gerilskog ratovanja, niti je to politički, niti ideološki pokret. To je metoda kojom određene grupe koje imaju neka svoja politička, filozofska ili religijska uvjerenja djeluju kako bi destabilizirale određenu zemlju ili regiju i kao bi na taj način promovorili svoja religijska, ekstremistička, radikalno marksistička, rasna ili fašistička uvjerenja.” (Vukadinović, R., 2007.)

Potencijal za katastrofalne terorističke napade koji pogađaju KI se konstantno povećava. Posljedice napada na industrijske upravljačke sisteme na

KI se mogu značajno razlikovati. Uobičajeno se pretpostavlja da bi uspješan cyber napad mogao prouzročiti malo žrtava, ako ih uopće bude, ali bi mogao dovesti do gubitka vitalne infrastrukturne usluge. Na primjer, uspješan cyber napad na javnu telefonsku komunikacijsku mrežu mogao bi oštetiti kupce telefonske usluge, dok tehničari resetiraju i popravljaju ovu KI. Napad na kontrolne sisteme postrojenja za kemikalije ili tečni prirodni plin mogao bi dovesti do šireg gubitka života kao i do značajne fizičke štete.[*]

Sagledavajući sve krivično-pravne aspekte složenosti pojma terorizma u međunarodnom i domaćem zakonodavnom pravu, možemo se složiti sa zaključcima objavljenim u publikaciji „Geopolitika“ u izdanju Akademiije Nauka i umjetnosti BiH, u kojoj se ističe: „Nema dileme da je terorizam, u svim svojim oblicima, vrlo izražena prijetnja i oblik ugrožavanja bezbjednosti ljudi i imovine. Zbog toga je neophodno određivanje takvih ponašanja kao krivičnih djela, propisivanje krivičnih sankcija za njihove učinioce, kao i uslova za njihovu primjenu prema učiniocima tih djela kako bi se obezbijedila zaštita najznačajnijih dobara i vrijednosti koje se ugrožavaju terorizmom i drugim krivičnim djelima povezanim sa njim. Ujedno, ovo je i obaveza koja proizilazi iz međunarodnih izvora koji obuhvataju terorizam i ponašanja u vezi sa njim. Uporedo s tim otvara se čitav niz izazova i dilema koje pred krivično zakonodavstvo postavljaju pitanje na koji način propisati odredbe i primijeniti ih prema učiniocima krivičnih djela. To je posebno izraženo kod onih inkriminacija koje kao radnje izvršenja propisuju radnje navođenja ili pripremne radnje. Tako se u pojedinim slučajevima može diskutovati o tome da li se radi o javnom podsticanju na terorizam ili slobodi izražavanja (kao garantovanom pravu) ili na koji način dokazati nekom licu da je učestvovalo u izvršenju terorističkih krivičnih djela u inostranstvu. Dakle, između propisivanja krivičnih djela terorizma i ponašanja koja su u vezi sa njim kao samostalnih krivičnih djela, garantovanja njihove primjene i zaštite osnovnih ljudskih prava – tanka je linija. Zbog toga je uloga krivičnog prava velika, te bi prednost trebalo dati stručnom razmatranju navedenih problema, analizi sudske prakse, te uvođenju međunarodnih odredaba putem internacionalizacije krivičnog prava, a ne pukom implementacijom usvojenih normi.

[*] Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism /* COM/2004/0702, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52004DC0702&from=HR (12.05.2021.)

Danas je „moderni terorizam“ usmjeren na destrukciju, slabljenje i uništenje KI kao „žile kucavice“ sasvremene društveno-političke zajednice. Teroristički napadi na objekte i sisteme KI, bez obzira da li se radi o „modernim cyber napadima“ na sisteme KI ili „tradicionalnim napadima eksplozivnim napravama“ na objekte KI, prijete ljudskim životima, materijalnim dobrima ali životnoj sredini, pa su jasna zakonska regulativa i rigorozne krivično-pravne sankcije ne samo potreba već i društvena obaveza, kako bi se oštro iskorijenila ili bar značajno oslabila ova pošast modernog društva.

3. KRIVIČNA DJELA KRAĐE U SISTEMIMA I OBJEKTIMA KRITIČNE INFRASTRUKTURE

Ova vrsta krivičnih djela se najčešće pojavljuje na objektima i sistemima KI, jer svojim pojedinačnim obimom ne prelaze neke značajnije iznose, a zbog razuđenosti i rasprostranjenosti objekata KI (saobraćajna, energetska, telekomunikaciona i sl.), bivaju teže uočavana i gotovo neprimjetna u odnosu na neke veće i značajnije ugroze KI (terorizam, sabotaže i dr.). Krivičnim Zakonom BiH se ne definiše pojam krađe, osim u smislu krađe naoružanja i vojne opreme, već je definicija te krivično-prvne radnja prepuštena entitetkim zakonima. Krivično djelo krađe se u članu 286. Krivičnog zakona Federacije BiH definiše kao protupravna radnja protiv imovine, odnosno ističe se da je krađa oduzimanje tuđe pokretne imovine od drugog lica s ciljem da se njenim prisvajanjem pribavi sebi ili drugom protupravu imovinsku korist.[*] U Krivičnom Zakoniku Republike Srpske, članom 224., pojam krađe je definisan kao oduzmanje tuđe pokretne stvari u namjeri da se ista protivpravno prisvoji.[*] A u članu 280. Krivičnog Zakona Distrikta Brčko, e definiše da ko tuđu pokretninu oduzme drugome s ciljem da njenim prisvajanjem pribavi sebi ili drugome protivpravnu imovinsku korist, počinio je krivično djelo krađe.

U sistemima i objektima KI, posebno u energetskom, telekomunikacionom i saobraćajnom sektoru, krađe opreme, dijelova i uređaja, predstavljaju čestu, gotovo svakodnevnu pojavu, jer su ovi sistemi meta

[*] Krivični Zakon Federacije Bosne i Hercegovine - Integralni tekst ("Službene novine Federacije BiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017)

[*] Krivični Zakonik Republike Srpske („Službeni glasnik RS", br. 64/2017, 104/2018 - odluka US i 15/2021)

kradljivaca sekundarnih sirovina (željezo, aluminij, plemeniti metali i sl.) Međutim počinioci ovih dijela ne razmišljaju o drugim dalekosežnijim i većim posljedicama, koje mogu izazvati otuđenje pojedinih elemenata u sistemima i objektima KI. Sofisticiranija verzija ovog krivičnog djela u odnosu na otuđenje sekundarnih sirovina, pojedinih elemenata, opreme i uređaja u sistemima i objektima KI, može biti organizovana krađa IT opreme i inovativnih tehnologija koje predstavljaju upravljačko srce KI od vitalnog značaja, a čije otuđenje može izazvati dugotrajne posljedice, prekide i uništenje direktno izložene KI, ali i drugih povezanih sistema.

Analizim aktuelnih krivičnih zakona na teritoriji Bosne i Hercegovine, uočavamo da se nigdje posebno ne tretira krivično pravna radnja krađe, koja za posljedicu ima i izazivanje drugih krivično pravnih radnji, kao što je npr. prekid rada sistema KI (npr. sistemi napajanja električnom energijom, saobraćajna infrastruktura i sl.). Krađe pojedinih elemenata i opreme na ovim i drugim sistemima KI, mogu izazvati teške posljedice po zdravlje i živote ljudi, imovinu i životnu sredinu, jer njihovim otuđenjem mogu nastati prekidi u snabdjevanju, odnosno mogu izazvati teže tehničko-tehnološke incidente sa daleko većim posljedicama. S toga ovakva krivična djela moraju biti prepoznata i primjenjena u nekim budućim unaprijeđenjima i ažuriranjima aktuelnih krivičnih zakona u Bosni i Hercegovini. Krivično pravne radnje krađe u sistemima i objektima KI, trebaju imati i regoroznije propisanu penalnu politiku odmjeravanja kazni, kako bi se suzbili negativni uticaji po širu društveno-političku zajednicu.

4. KRIVIČNA DJELA SABOTAŽE U SISTEMIMA I OBJEKTIMA KRITIČNE INFRASTRUKTURE

Pojam sabotaže je prepoznat u Krivičnom Zakonu Federacije BiH, samo kao pojam „računalne sabotaže“ koji definiše tu radnju kao unos, izmijenu, brisanje ili prikrivanje računalnih podataka ili programa ili se na neki drugi način vrši uticaj na računalni sisteme, ili uništenje ili oštećenje naprava za elektronsku obradu podataka s ciljem da se onemogući ili znatno omete postupak elektronske obrade podataka značajnim organima vlasti, javnim službama, javnim ustanovama, trgovačkim društvima ili drugim pravnim osobama od posebnog javnog interesa, pa time prouzrokuje štetu u iznosu većem od 500.00 KM. Članom 290. Krivičnog Zakonika Republike Srpske se definiše pojam sabotaže kao namjera ugrožavanja ustavnog uređenja ili

bezbjednosti Republike Srpske na prikriven, podmukao ili drugi sličan način, u vršenju svoje službene dužnosti ili radne obaveze, kojom se prouzrokuje znatnu štetu za organe Republike Srpske ili pravno lice u kojem radi ili za drugi organ Republike Srpske ili pravno lice. Također i u Krivičnom Zakonu Distrikta Brčko u članu 392. se pojam sabotaže definiše kao i Krivičnom zakonu Federacije BiH, kao pojam računarske sabotaže.

Dakle, možemo zaključiti da je sabotaža oblik subverzije koji uključuje namjernu štetu, ometanje ili ometanje nečega putem određenih radnji: štrajkova, obustava rada, mitinga, računarskih i drugih oblika zaustavjanja radnih i tehnoloških procesa. Sama riječ „sabotaža“ ima francuske korijene i prema narodnom govoru taj izraz potiče od prakse bacanja drvenih cipela u XIX vijeku, poznatih kao "sabot", u industrijske razboje za vrijeme industrijske revolucije. Razlog za ovu pojavu bila je pojava novih automatiziranih mašina, što je zauzvrat dovelo do velikog smanjenja broja radnika. Ne smišljajući ništa razumnije, radnici koji nisu željeli izgubiti izvor prihoda jednostavno su razbili opremu bacajući drvene cipele u mehanizme. Postoji mnogo različitih oblika sabotaže, koji su svi dizajnirani da na neki način ometaju aktivnosti i stvaraju kaos. Sabotaža predstavlja i namjerno zaustavljanje i opstrukcija nečijih dužnosti uz prethodni dogovor. Na ruskom jeziku, od ove riječi nastao je glagol "sabotaža", koji se odnosni na neispunjavanje dužnosti ili njihovo nasumično izvršavanje u znak protesta, na primjer, protiv loših uslova rada ili kašnjenja u platama. U SSSR-u je sabotaža bila krivično djelo, za čije se sprečavanje predvižala i upotreba vatrenog oružja. Unutrašnje sabotaže su najčešće izazvane štrajkovima i obustavama rada koji mogu imati različite povode kako one „opravdane“ u borbi za boljim uslovima rada, tako i one „subverzivne“ koji najčešće dolaze izvana i za cilj imaju slabljenje, prekid ili uništenje sistema KI. Najupečatljivije vrste sabotaže izazvanih različitim neprijateljskim povodima i djelovanjima izvana, su: vojne, industrijske i ekološke.

Vojne sabotaže koje se izvode putem različitih diverzija, se smatraju najopasnijim neprijateljskim atakom na sisteme i objekte KI kao žile kucavice državnog ustavno-pravnog poretka. Tokom svojih subverzivnih aktivnosti, diverzanti se infiltriraju u neprijateljsku odbranu KI i pokušavaju uništiti sisteme proizvodnje naoružanja, infrastrukturu i sisteme opskrbe. Ova vrsta sabotaže može imati i politički oblik, odnosno za cilj imati nasilnu promjenu društveno-političkog uređenja. U ovom slučaju, diverzanti, najprije šire

namjerno lažne vijesti i glasine a zatim vrše sabotaže na sistemima, najčešće organizujući štrajkove i prekide tehnoloških procesa.

Industrijska sabotaža su uglavnom povezane sa finansijskim ciljevima i najčešće su povezane sa krađom intelektualnog vlasništva koja za cilj ima stvaranje prednosti nad tržištem i stvaranje monopola na određene usluge i proizvode. Tokom nadmetanja za tržište, među konkurentima se poduzimaju sabotažne djelatnosti, najčešće širenjem glasina i lažnih optužbi, kako bi se po svaku cijenu ometala konkurencija, a što svakako utiče i na samu proizvodnju i tehnološki proces određene KI.

Ekološke sabotaže najčešće uključuju radnje izvedene s ciljem oštećenja opreme koja se koristi u ekološki opasnim aktivnostima i na ekološki osjetljivim KI, kao što su proizvodnja opasnih i štetnih materija. Na ovaj način se subverzivnim djelatnostima, iznutra i izvana, izazivaju ekološki incidenti i katastrofe koji su opasni po živote i zdravlje ljudi, te floru i faunu u određenom području.

Moderne sabotaže današnjice se rade vanjskim i unutrašnjim cyber napadima na upravljačke procese i IT sisteme KI. Mnogo je primjera ovakvog subverzivnog djelovanja u poslednjem desetljeću, a najupečatljiviji se odvijao na početku otovorenog Rusko-Ukrajinskog sukoba, koji potresa Evropu u poslednjih 5 godina. 23.12.2016. oko 17 sati na stranicama kompanije za distribuciju električne energije „Prykarpattyaoblenergo“, koja je klasifikovana KI u zapadnoj ukrajinskoj regiji Ivano-Frankivsk, pojavila se obavijest da je glavni grad te regije ostao bez električne energije i poruka građanima da ne kontaktiraju službu za korisnike. (Lambaša, B., 2021.) U tom trenutku još nije bilo nikakvih detalja o samom uzroku nestanka električne energije. Nakon samo pola sata stigla je informacija iz komapnije da je bez energije ostala cijela regija, a već u sljedećem saopćenju je jasno rečeno da su problem izazvali vanjski akteri koji su preuzeli kontrolu nad upravljanjem sistema. Otprilike u isto vrijeme i druga velika ukrajinska kompanija iz energetskog sektora, „Kyivoblenergo“, objavila je da je hakirana te da su napadači preuzeli kontrolu nad sistemom čime je bez električne energije ostalo 80.000 stanovnika. Kao i u prvom slučaju, služba za korisnike bila je preplavljena telefonskim pozivima što je uzrokovalo kompletan pad sistema korisničke službe. Zanimljivo je da su brojni pozivi stizali iz inostranstva, dakle, nisu zvali ljudi koji su ostali bez električnog napajanja. Naime, pozivanjem službe za korisnike napadači su srušili i taj ssistem koji je u tim trenucima bio od izuzetne važnosti i tako korisnicima sinkronizirano uskratili dvije usluge, opskrbu i informaciju. To je

bio povod za širenje glasina i straha na tom području. Tek nakon opsežne istrage koja je trajala nekoliko tjedana počeli su polako pristizati u javnost detalji o incidentima. Izvorni napad onesposobio je upravljačke sklopove u postrojenjima čime je postignut primarni cilj - nestanak električne energije. Kako bi osigurali što kasniju reakciju, napadači su izveli napad na nadzorne sisteme koji su tokom nestanka energije uredno prikazivali stanje kao normalno. Osim tog napada koji je prouzročio najveću štetu, izveden je i (telefonski) DoS napad na korisničku službu kompanija, a nakon toga i napad na poslovnu mrežu. Forenzičkom analizom nakon napada u poslovnim mrežama kompanija pronađen je zloćudni kod KillDisk čije su komponente zadužene za brisanje najvažnijih sistemskih datoteka što onemogućuje ponovno pokretanje računala i poslužitelja. U isto vrijeme je napadnuto 6 elektrana širom Ukrajine. Pojedinačno nijedan napad nije sofisticiran, međutim uspješna sinhronizacija napada ukazuju na visok stepen tehničkih vještina napadača.

Za razliku od ukrajinskih elektrana u kojima je došlo do prekida isporuke električne energije, u njemačkom je slučaju napada na jednu neimenovanu čeličanu, došlo do fizičkog uništenja dijela postrojenja. Iako detalji nisu poznati u javnosti, šteta je navodno značajna, a vektor inicijalne zaraze je sličan kao i u ukrajinskom slučaju. Naime, nekoliko mjeseci prije incidenta potvrđen je „spear phishing“ napad kojim je zlonamjerni kod ušao u poslovnu mrežu kompanije. U velikim industrijskim postrojenjima često je problem da poslovne mreže nisu na primjeren način odvojene od procesnih mreža koje služe isključivo za upravljanje i nadzor nad postrojenjima. Primjeran način odvajanja bi bila potpuna izolacija tih dviju mreža kako bi se jednostavno izbjegle sve opcije pristupa iz jedne mreže u drugu i obratno. Nažalost, iz praktičnih razloga mreže su najčešće povezane u uskom segmentu koji se nakon incidenta pokaže dovoljno širokim za kompromitaciju sistema. Baš to se dogodilo i u njemačkoj čeličani – maliciozni kod je e-mail porukom ušao u poslovnu mrežu iz koje je pronašao put do procesne mreže. Softverskim gašenjem sigurnosnih mehanizama postrojenje nije ispravno odreagiralo na mehaničke poteškoće i došlo je do fizičke štete. Definitivno najpoznatiji napad na industrijska postrojenja je onaj malicioznim kodom „Stuxnet“ na nuklearno postrojenje Natanz u Iranu. „Stuxnet“ je maliciozni kod visokog stepena složenosti koji je djelovanjem na SCADA komponente iranskog nuklearnog postrojenja uspio fizički uništiti brojne centrifuge za obogaćivanje urana i time unazaditi iranski nuklearni program. Iako se napad dogodio prije više od šest

godina sve komponente tog koda do danas nisu potpuno analizirane. Priznanje za razvoj i upotrebu tog moćnog oružja nikad nije stiglo iako se nagađa da iza njega stoje dvije najveće svjetske cyber-sile SAD i Izrael. Upravo su SAD domovina prvog pravog iako insceniranog cyber-napada na industrijske uređaje. Ono što danas poznajemo pod imenom „Aurora Generator Test“ provedeno je 2007. godine u „Idaho National Laboratory“ u svrhu demonstracije mogućnosti fizičkog uništenja uređaja pomoću cyber-oružja.

Sabotaže mogu biti izazvane s umišljajem i direktnom namjerom ali i iz nehata, nesavjesnim ponašanjem i radnjama unutar tehnoloških procesa u sistemima i na objektima KI. Primjetno je da ovi krivično-pravni aspekti nisu dovoljno istraženi, niti su jasno definisani zakonodavno krivičnim regulativama kako na međunarodnom polju, tako i unutar Bosne i Hercegovine. Svjedoci smo čestih prekida lanaca dobave u sistemima KI (prekid napajanja strujom, vodom, gasom, lijekovima i sl.) a da se nikada ne utvrdi krajnja odogovornost niti se sankcionišu ovakve detruktivne i krivičnno-pravno kažnjive radnje. Potrebno je bližoj budućnosti unaprijediti krivični zakon sa ovim aspektima, kako bi se preventivno uticalo na efikasniiju zaštitu sistema KI i njihovih konzumenata.

5. KRIVIČNA DJELA ŠPIJUNAŽE U SISTEMIMA I OBJEKTIMA KRITIČNE INFRASTRUKTURE

Krivičnim Zakonom BiH u članu 163 je definisano krivično djelo špijunaže: (1) Ko tajne podatke saopšti, preda ili učini dostupnom stranoj državi, stranoj organizaciji ili licu koje im služi, kazniće se kaznom zatvora od jedne do deset godina. (2) Ko na štetu Bosne i Hercegovine za stranu državu ili organizaciju stvara obavještajnu službu u Bosni i Hercegovini ili njom rukovodi, kazniće se kaznom zatvora najmanje pet godina. (3) Ko stupi u stranu obavještajnu službu, prikuplja za nju podatke ili na drugi način pomaže njen rad, kazniće se kaznom zatvora od jedne do deset godina. (4) Ko pribavlja tajne podatke u cinju da je saopšti ili preda stranoj državi, stranoj organizaciji ili licu koje im služi, kazniće se kaznom zatvora od jedne do deset godina. (5) Ko nabavlja sredstva za učinjenje krivičnog djela iz stava (1) i (2) ovog člana, kazniće se kaznom zatvora od jedne do deset godina.

Ova vrsta krivičnih dijela na sistemima KI je najčešće povezana sa cyber sigurnošću upravljačkih modula na složenim i vitalnim KI, kao što su

energetska, telekomunikaciona, odbrambena, finansijska i sl. Krivična djela špijunaže se u današnje moderno doba vežu za hakerske napade i pokušaje napadača da prije nego što subverzivnim dejstvima sabotaže i diverzije izvrše onesposobljavanje istema KI, najprije izvrše djela špijunaže a zatim i krađe određenih značajnih informacija i intelektualnog vlaništva. Dakle, krivična djela špijunaže predhode krivičnim djelima krađe i sabotaže u cilju prikrivanja ovih krivičnih djela, te se zajedno mogu smatrati multiugrozima sistema zaštite KI. Ovakav složeni hazard zahtjeva i posebno sofosticirni pristup, te angažman obavještajne zajednice u preventivnoj zaštiti sistema KI. Pravovremeno prikupljanje operativnih podataka o kretanjima bezbjednosno-interesantnih lica ili grupa koje za cilj imaju sisteme KI kao mete napad na ustavni i društveno-politički poredak, je od ključne važnosti za efikasnu zaštitu sistema KI.

Cyber špijunaža je upotreba elektroničkih mogućnosti za ilegalno prikupljanje informacija od cilja. Za sve nacije, revolucija informacione tehnologije tiho je promijenila način rada vlada. Asimetrična prijetnja koju predstavljaju cyber napadi i inherentne ranjivosti cyber prostora predstavljaju ozbiljan sigurnosni rizik s kojim se suočavaju sve nacije. Postignuća cyber špijunaže - na koja su organi reda i kontraobavještajni rad pronašli malo odgovora - nagovještavaju da su ozbiljniji cyber napadi na kritične infrastrukture samo pitanje vremena (Geers 2010). Ipak, planeri nacionalne sigurnosti trebali bi se svim prijetnjama baviti metodom i objektivnošću. Kako ovisnost o IT-u i Internetu raste, vlade bi trebale ulagati proporcionalno u mrežnu sigurnost i odgovor na incidente na cyber špijunaže (Geers 2010; Lehto 2013).

Rizik od špijunaže je aktualan i konkretan za sve organizacije širom svijeta, kako u privatnom tako i u javnom sektoru. A glavni pokretač ove prijetnje je sve veće oslanjanje na internet računarske sisteme za pohranjivanje, obradu i razmjenu informacija od ključne važnosti za poslovanje digitalne informacije preko organizacijskih granica i povećanje telekomunikacije putem Interneta. Ovi trendovi iznjedrili su novi i specifični izraz za rizik koji povjerljive informacije vanjski kriminalci mogu ugroziti ili ukrasti: „E-špijunaža“. Svake minute svakog dana, sve veći broj dobro raspoloženih resursa i visoko-sofisticirani cyber kriminalci iz cijelog svijeta žele steći neovlašteni pristup vrijednim podacima koje posjeduju kompanije i vlade.

Krajem 2007., Jonathan Evans - generalni direktor MI5, Britanske kontra-obavještajne službe, kojoj je odgovoran 2UK centar za zaštitu

nacionalne infrastrukture (CPNI)“, poslao povjerljivo pismo na adrese 300 Britanskih poslovnih lidera u bankama, računovođama i pravnim agencijama, upozoravajući ih na koordiniranu kampanju „e-špijunaže“, zasnovane na neprijateljskoj mreži protiv Britanske ekonomije. MI5 ističe na svojoj web stranici: „Obavještajne aktivnosti pogađaju komercijalne organizacije mnogo više nego što je to bilo u prošlosti.”

Uprave imaju tendenciju da vode računa o sigurnosti i integritetu svojih korporativnih podataka kao sastavnim dijelovima svojih IT sistema. Međutim, sve veća prijetnja i rastući utjecaj mogućih špijunskih prodora, zahtjevaju pojačanu prevenciju i otkrivanje „e-špijunaže“ u ranoj fazi kako bi se preventivno zaštitili sistemi KI. Ovakav prostup bi trebao biti na dnevnom redu svakog menadžmenta KI. Oni koji se ne usredotoče na to, izlažu se riziku za samu budućnost svojih sistema. Da bi se brzo procijenila spremnost i sposobnost vašeg preduzeća da upravlja rizikom „e-špijunaže“, potrebno je odogovriti na nekoliko ključnih pitanja, poput: 1) Da li je prijetnja „e-špijunažom“ u vašem registru korporativnih rizika da li o tome raspravljate u vašim godišnjim izvještajima? 2) Znate li koliko ste sigurnosnih incidenata pretrpjeli u proteklih godinu dana i kakva je priroda tih incidenata? 3) Pratite li svoje informacijske sisteme i njihovu izloženost 24 h dnevno, 7 dana u tjednu? 4) Imate li sigurnosnu strategiju i pristup upravljanja koji je usklađen sa vašom poslovnom strategijom?

Ako je bilo koji od odgovora „ne“ onda se organizacija mora ozbiljno pozabaviti ranjivošću svoga sistema i angažovati neovisne vanjske stručnjake za procjenu ugroženosti i prijedloge mjera za unaprežđenje zaštite sistema KI od špijunaže.

6. ZAKLJUČAK

Kada je rječ o krivično-pravnim aspektima zaštite KI, a posebno krivičnih djela terorizma, krađe, sabotaže i špijunaže, kao najčešćih pojavnih oblika „modernih“ ugroza sistema KI, onda posebnu pažnju treba obratiti na preventivne mjere njihovog ranog otkrivanja, ali i unaprijeđenje zakonodavnog okvira u smislu preciznijeg definisanja ovih krivičnih dijela i pooštravanja krivičnih sankcija za ovakvu vrstu prijetnji po vitalne sisteme KI. Ove mjere mogu sadržavati, pored standardnih krivično-pravnih akcija i aktivnosti usmjerene na određene edukativno-marketinške kampanje

odvraćanja od namjera i različitih društveno-političkih ili kriminalnih motiva ugroza sistema i objekata KI.

Teroristički napadi na objekte i sisteme KI, mogu biti „moderni cyber napadi“ na sisteme KI ili „tradicionalni napadi eksplozivnim napravama“ na objekte KI. Uticaji terorističkih napada prijete ljudskim životima, materijalnim dobrima i životnoj sredini, pa je potrebno unapređenje zakonske regulative i krivično-pravnih sankcija, kako bi se oštrije iskorijenila ili bar značajno oslabila ova bolest modernog društva.

Krađe elemenata i opreme na sistemima i objektima KI, mogu izazvati teške posljedice po zdravlje i živote ljudi, imovinu i životnu sredinu, jer njihovim otuđenjem mogu nastati prekidi u snabdjevanju. Odnosno ovakve krivično-pravne radnje mogu izazvati i teže tehničko-tehnološke incidente sa daleko većim posljedicama, pa trebaju imati i regoroznije propisanu penalnu politiku odmjeravanja kazni, kako bi se suzbili negativni uticaji po širu društveno-političku zajednicu.

Krivično-pravni aspekti sabotaže nisu jasno definisani zakonodavno-krivičnomm regulativom. Sabotažama se prekidaju lanci dobave u sistemima KI (prekid napajanja strujom, vodom, gasom, lijekovima i sl.), te određivanje krajnje odogovornosti predstavlja veoma složen proces dokazvanja. Potrebno je unaprijediti krivični zakon i preciznije definisati ove aspekte, kako bi se preventivno uticalo na efikasniiju zaštitu sistema KI i njihovih konzumenata.

Krivična djela špijunaže predhode krivičnim djelima krađe i sabotaže, koje se vrše najčešće u cilju prikrivanja predhodnih krivičnih djela, te se zajedno mogu smatrati multiugrozima sistema zaštite KI. Ovakav složeni hazard zahtjeva i posebno sofisticirni pristup, te angažman obavještajne zajednice u preventivnoj zaštiti sistema KI.

Sagledavajući sve aspekte složene krivično-pravne problematike u pogledu njene definicije, krivično procesnih radnji, kao i krivičnih sankcija i mjera koje trebaju preventivno zaštiti i odvratiti potencijalne buduće počinitelje različitih vrsta ugroza u sistemima i na objektima KI, možemo zaključiti da su potrebni dodatni napori akademske zajednice i struke da se preciznije obrade svi krivično pravni aspekti zaštite sistema KI. Posebno se trebaju iznaći unapređenja u pogledu multihazarda i povezanosti određenih krivičnih djela, kao što su špijunaža, krađa i sabotaža.

LITERATURA

1. Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism /* COM/2004/0702, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52004DC0702&from=HR
2. Cvjetković, B.,: Terorizam- sredstva i posljedice, Split, Kupo1a Laus, 2002.,
3. Harmon, C., (202).Terorizam danas, Zagreb, Golden marketing,
4. Kešetović, Ž., Korajlić, N., Toth, I., (2013). Krizni menadžment. FKKSS, Univerzitet u Sarajevu i Veleučiliste Velika Gorica.
5. Klaić, B., (1978). „Terror“, u: Rječnik stranih riječi, Zagreb, Nakladni zavod Matice Hrvatske,
6. Korajlić, N i sar., (2012). Istraživanje krivičnih djela. Pravni fakultet Univerziteta u Sarajevu,
7. Korajlić, N., Selimić, M.. (2015). Kriminalistička taktika. Visoka škola „CEPS – Centar za poslovne studije“ Kiseljak,
8. Krivični Zakon Federacije Bosne i Hercegovine, Integralni tekst ("Službene novine Federacije BiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017)
9. Krivični Zakonik Republike Srpske, („Službeni glasnik RS", br. 64/2017, 104/2018 - odluka US i 15/2021)
10. Lambaša, B., (2021). „Open Info Trend“, Informatički online magazin, Zagreb,
11. PricewaterhouseCoopers LLP, „E-espionage - What risks does your organisation face from cyber-attacks?“, 2011,
12. Reosiguravajuća kuća Munich RE, NatCatSERVICE, https://natcatservice.munichre.com/ (pristup: 12.07.2021.)
13. Rezolucija Generalne skupštine UN-a 56/195, Mandat UNDRR-a
14. Simović, M., Šikman, M., (2017). „Krivičnopravna zaštita od terorizma (međunarodni standardi i pravni okvir u Bosni i Hercegovini), Akademija Nauka i umjetnosti BiH,
15. UN DRR Global Assesment Report, https://gar.undrr.org/sites/default/files/reports/2019-05/full_gar_report.pdf

16. Vigano, E., Loi, M., Yaghmaei, E., (2020). „Cybersecurity of critical infrastructure“, Springer,
17. Vukadinović, R., (2004). Međunarodni politički odnosi“, Zagreb, Politička kultura,
18. Wise, R., J., (2020). „Terrorism and Homeland Security -Ninth Edition“.